## REMARKS/ARGUMENTS

Reconsideration of the application is requested.

Claims 1-13 remain in the application. Claims 1, 6, 7, and 9-13 have been amended.

With regard to paragraph 1 on page 2 of the Office action, enclosed herewith is an added drawing figure illustrating the method of claim 6. The labels and the flow of Fig. 10 are supported in the original claim 6 and in the specification as a whole. Further, the added brief description and the added detailed description of Fig. 10 are supported in claim 6 of the original application.

With regard to paragraphs 2 - 4, the Abstract of the Disclosure has been amended by shortening the same and by removing "Fig. 2" from the Abstract page.

The specification and the claims meet the requirements of 35 U.S.C. § 112, first and second paragraphs. The drawing meets the requirements of 37 CFR §§ 1.83 and 1.84. Should the Examiner find any further objectionable items, counsel would appreciate a telephone call during which the matter may be resolved.

We now turn to the art rejection, in which claims 1, 2, 4, 5, 7, and 8 have been rejected as being obvious over Sedlak (US 4,870,681) in view of Guido van Rossum (*"Guido"*) under 35 U.S.C. § 103. We respectfully traverse on the basis of the amended claims.

Before delving into the details of the teachings found in the prior art references, it appears that a brief review of the invention - in terms of a general juxtaposition between the claims and the primary reference Sedlak - is in order.

The presently claimed invention relates to a situation in which the multiplicand, the multiplier and the modulus are polynomials of a variable rather than integers. While Sedlak only relates to integers in an integer modulo arithmetic, the present invention relates to polynomials of variable in polynomial modulo arithmetic. Claim 1 has been amended to further emphasize the polynomial characteristic, as opposed to the integer characteristic. It should be noted, however, that this characteristic was already contained in the claims and, as such, the claim has not been narrowed by any substantial reason related to the statutory requirements for a patent.

Support for the added wording in claim 1 is found in the specification, page 30, fifth paragraph.

The differences between the integer arithmetic or Z/NZ arithmetic and the polynomial modulo arithmetic or a GF($2^n$) arithmetic are discussed in detail on pages 1 to 4 of the specification. In the integer arithmetic, one simply has integer numbers, while polynomial modulo arithmetic is characterized by polynomials of a variable x, wherein the polynomial is further characterized by coefficients $a_i$ of the polynomial terms, which are different powers of the variable x.

In the Examiner's summary of Sedlak, the latter is alleged to teach "multiplicand, multiplier and modulus being polynomials of a variable." This is patently incorrect. Instead, Sedlak only relates to integers. Sedlak's members of the multiplication are not polynomials.

As noted above, we have even further emphasized this difference, by stating that we deal with polynomials of a variable in a polynomial modulo arithmetic.

With specific reference to the wording of claim 1. Sedlak is different from claim 1 for the following reasons:

In method steps (d), (c), (d), (e), (f), several polynomials of the variable x are cited.

In contrast, Sedlak is completely silent with regard to polynomials. As indicated above, this is not surprising, since Sedlak is only related to an integer arithmetic algorithm.

Additionally, and importantly, step (c) of claim 1 states that, in accordance with the present invention, the reduction shift value is equal to the difference of the decree of the shifted intermediate result polynomial and the degree of the modulus polynomial. This means that the inventive device has a very easy calculation of the reduction shift value. It can simply be calculated by looking at the degree of the shifted intermediate result polynomial and the degree of the modulus polynomial and by calculating the difference between these degrees. As it is outlined in the first two lines of page 2 of the specification, the highest power of the variable x is called the degree of the polynomial. Therefore, it becomes clear that the degree of the polynomial can be determined very easily. To summarize, the calculation of the reduction shift value in the reduction look-ahead method as defined in step (c) of claim 1 is very easy and can be implemented in an arithmetic unit very efficiently.

This is, however, completely different in Sedlak. The calculation of the reduction shift value sn in Sedlak is described in detail in column 16, to wit:

> Carry out the following, if and only if Z≤ZDN:
> (a) Set sn:= 0.
> (b) Set n:= n-1 and
> (c) Shift ZDN 1 bit rightward, i.e. divide ZDN by 2.

Sedlak, col. 16, lines 51 to 54. That is, first of all, the value ZDN has to be calculated. ZDN stands for "Zwei Drittel N", which translates into English as "two thirds of N".

That is, to perform the Sedlak method, the reduction look-ahead method firstly has to calculate the value of ZDN (column 17, lines 3 and 4). This calculation, i.e., multiplying a number by the factor 2/3 is a very difficult process for efficient implementation. Then, the time-consuming iterative algorithm in column 16, lines 51 - 54 has to be calculated to finally obtain the reduction shift value. Thus, the Sedlak method (for the integer arithmetic) includes the time-consuming steps of calculating the value of ZDN and the subsequent iterative algorithm of the foregoing paragraph (col. 16, lines 51-54).

Contrary thereto, the inventive method for the polynomial modulo arithmetic simply performs the calculation of the difference of the degree of the shifted intermediate result polynomial and the degree of the modulus polynomial. In the inventive method as becomes clear from step (c) in claim 1, no ZDN calculation or no iterative algorithm are necessary.

It is quite clear that the Examiner's comments in the paragraph bridging pages 3 and 4 of the Office action, in which the Examiner asserts that this step is shown in Sedlak, are in error. The Examiner compares the value sn in Fig. 6b of Sedlak to the reduction shift value as defined in claim 1. Unfortunately, the Examiner does not provide any source for the rather "cryptic" statement in the brackets in the second and third lines of page 4 of the Office action. Specifically, we cannot find the variable k or the variable "minus k" in Fig. 6 or the corresponding description of Fig. 6, in col. 16-17 of Sedlak. The Examiner is respectfully urged not to overlook the teaching in Sedlak's col. 16, lines 51 - 54 (see above), where the determination of the reduction shift value sn is described in detail. The Examiner is urged to reconsider the comments with regard to step (c).

We now turn to the secondary reference *Guido* and to the Examiner's remarks concerning steps (b) and (d) in relation with *Guido*. The only pertinent statement that we find in the reference is the rather fleeting remark that "left-shift [can be interpreted] as multiplication by a power of 2," that is a multiplication of a number by a power of 2 is equivalent to a left-shift of a binary number (in a register). However, steps (b) and (d) of claim 1 do not require raising the number "2" to the power of the multiplication shift value. Instead, these steps state that the variable of the polynomials has to be raised to the power of the multiplication shift value or the reduction shift value. More importantly, however, it is clear that *Guido* does not make up for the short-coming of the primary reference Sedlak concerning the lack of the polynomial multiplication.

Concerning the rejection of claims 3 and 9, we have also reviewed the third reference to Dodson et al. (US 5,251,164), and we find this reference does not save the error in the rejection either. That is, the teaching Dodson et al. does not make up for the above short-coming of the primary reference.

In summary, none of the references, whether taken alone or in any combination, either show or suggest the features of claim 1. Claim 1 is, therefore, believed to be patentable over the art and since all of the dependent claims are ultimately dependent on claim 1, they are believed to be patentable as well.

In view of the foregoing, reconsideration and allowance of claims 1-13 are solicited.

If an extension of time for this paper is required, petition for extension is herewith made.

Respectfully submitted,

For Applicants

WERNER H. STEMER
REG. NO. 34,956

WHS:tk

September 24, 2004

Lerner and Greenberg, P.A.
P.O. Box 2480
Hollywood, Florida 33022-2480
Tel.: (954) 925-1100
Fax: (954) 925-1101